

State of Vermont
Agency of Digital Services
Secretary's Office
109 State Street, 5th Floor
Montpelier, VT 05609-2001

John Quinn III, State CIO & Secretary
Shawn Nailor, Deputy Secretary

[phone] 802-828-4141

MEMORANDUM

TO: All Executive Branch Agencies, Departments, and Offices

FROM: John Quinn, Secretary, Agency of Digital Services



DATE: February 19, 2019

SUBJECT: Cybersecurity Standard Update 19-01

References:

- a) 3 V.S.A. § 2283(b)
- b) 3 V.S.A. § 2222(a)
- c) Department of Homeland Security Binding Operational Directive 01-17
- d) John S. McCain National Defense Authorization Act for Fiscal Year 2019
- e) 2019 Worldwide Threat Assessment of the US Intelligence Community

Cybersecurity Standards issued by the Agency of Digital Services (ADS) are direction to all executive branch State Agencies pursuant to References (a) and (b) for the purposes of safeguarding State of Vermont information and information systems. "State Agency" as used in this Standard shall include all State agencies, departments, commissions, committees, authorities, divisions, boards or other administrative units of the Executive Branch.

Background:

The ever-evolving nature of cyber threats has continued to prove that the State of Vermont and the valuable data that we hold for our citizens is a priority target for cyber criminals and hackers alike. The Agency of Digital Services (ADS) has determined that the risks presented by Kaspersky-branded products or services, and covered telecommunications equipment or services including those provided by Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company justify issuance of this Cybersecurity Directive.

The federal cybersecurity and intelligence communities have documented evidence of the concerns regarding these products or telecommunications equipment and have used several



mechanisms, including References (c) and (d), to block their use within the federal technology community. These concerns include:

1. The broad access to files and elevated privileges of anti-virus software, including Kaspersky software; ties between Kaspersky officials and Russian government agencies; and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting between Kaspersky operations in Russia and Kaspersky customers, including government customers in the United States.
2. The US Intelligence Communities' assessment, cited in Reference (e), expressing concern "about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies."

Updates:

1. Effective immediately the acquisition, renewal of contracts, or use for a new purpose of Kaspersky-branded products on all State of Vermont information systems, or any vendor system, is prohibited. No current use of these products will continue beyond the dates provided in Cybersecurity Directive 19-01, except as provided therein.
 - a. "Kaspersky-branded products" means information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates, including Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc. (collectively, "Kaspersky"), including those identified below.
 - b. Kaspersky-branded products currently known to ADS are: Kaspersky Anti-Virus; Kaspersky Internet Security; Kaspersky Total Security; Kaspersky Small Office Security; Kaspersky Anti Targeted Attack; Kaspersky Endpoint Security; Kaspersky Cloud Security (Enterprise); Kaspersky Cybersecurity Services; Kaspersky Private Security Network; and Kaspersky Embedded Systems Security.
2. Effective immediately, the acquisition, renewal of contracts, or use for a new purpose of equipment manufactured by the companies listed in paragraph 2.a that is supporting any State of Vermont information systems, or any vendor system, is prohibited. No current use of these products will continue beyond the dates provided in the requirements outlined in Cybersecurity Directive 19-01.
 - a. Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company. This includes equipment used to support any information technology, telecommunications, industrial control system, supervisory control and data acquisition system, systems used for the purpose of public safety,



security of government facilities, physical security surveillance of critical infrastructure, and other security purposes, building infrastructure support, or video surveillance purpose.

3. Any request for exception to this Standard will be considered on a case-by-case basis, submitted with a plan of action with milestones for transition away from the prohibited items, by the Secretary of Digital Services after receiving a request, endorsed by the Secretary of the requesting State Agency and the Chief Information Security Officer, articulating the compelling justification for additional time to implement the requirements.
4. Nothing in this standard shall be construed to endorse or permit any current use of these technologies.
5. Internal point of contact for this Directive is Nicholas Andersen, State of Vermont Chief Information Security Officer, at nicholas.andersen@vermont.gov.



State of Vermont
Agency of Digital Services
Secretary's Office
109 State Street, 5th Floor
Montpelier, VT 05609-2001

John Quinn III, State CIO & Secretary
Shawn Nailor, Deputy Secretary

[phone] 802-828-4141

MEMORANDUM

TO: All Executive Branch Agencies, Departments, and Offices

FROM: John Quinn, Secretary, Agency of Digital Services

DATE: February 19, 2019

SUBJECT: Cybersecurity Directive 19-01

References:

- a) Cybersecurity Standard Update 19-01

Cybersecurity Directives issued by the Agency of Digital Services (ADS) are direction to all executive branch State Agencies for the purposes of safeguarding State of Vermont information and information systems. "State Agency" as used in this Directive shall include all State agencies, departments, commissions, committees, authorities, divisions, boards or other administrative units of the Executive Branch. This Directive provides actions associated with Cybersecurity Standard Update 19-01.

Required Actions:

1. Within 30 calendar days after issuance of this directive, identify the use or presence of Kaspersky-branded products on all information systems and provide to ADS, via the relevant Agency Information Technology (IT) Leader, a report that includes:
 - a. A list of Kaspersky-branded products found on any State Agency systems, or in use by any State of Vermont vendor on a system that transmits, stores, or interacts with State of Vermont systems or data. If State Agencies do not find the use or presence of Kaspersky-branded products on their information systems, inform ADS that no Kaspersky-branded products were found.
 - b. The number of endpoints impacted by each product, and
 - c. The methodologies employed to identify the use or presence of the products.



2. Within 30 calendar days after issuance of this directive, identify the use or presence of any of the identified covered telecommunications equipment and provide to the Chief Information Security Officer (CISO), via the relevant Agency Information Technology (IT) Leader, a report that includes:
 - a. A list of any of the telecommunications products listed in Cybersecurity Standard 19-01 found supporting any State Agency, or in use by any State of Vermont vendor to transmit, store, or interact with State data or information. This includes equipment used to support any information technology, telecommunications, industrial control system, supervisory control and data acquisition system, systems used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other security purposes, building infrastructure support, or video surveillance purpose.
 - b. The number of endpoints impacts by each product, and
 - c. The methodologies employed to identify the use or presence of the products.
3. Within 60 calendar days after the issuance of this directive, a follow-up report shall be provided to the CISO, via the relevant Agency IT Leader, that identifies any additional information discovered as an update to the 30-day report and the following information:
 - a. List of agencies, departments, or offices impacted;
 - b. Mission function of impacted endpoints, systems, telecommunications equipment or devices;
 - c. All contracts, service-level agreements, or other agreements entered into with any vendor that supplies or uses the products, services, or telecommunications equipment outlined in this Directive;
 - d. Timeline to remove the identified products, services, or telecommunications equipment;
 - e. Performance or security impacts of removing the identified products, services, or telecommunications equipment;
 - f. If applicable, chosen or proposed replacement products/capabilities;
 - g. If applicable, timeline for implementing replacement products/ capabilities;
 - h. Anticipated challenges not otherwise addressed in this plan; and
 - i. Associated costs related to licenses, maintenance, and replacement;



4. Within 90 calendar days after the issuance of this directive, unless otherwise approved or directed by ADS based on new information, begin to implement the agency plan of action and provide a status report to ADS on the progress of that implementation every 30 calendar days thereafter until full removal and discontinuance of use is achieved.
5. These reporting requirements extend to all State of Vermont information technology vendor systems and/or telecommunications infrastructure. No State Agency shall procure or obtain or extend or renew a contract to procure or obtain any service or systems that use any product, service, system, or equipment referenced within this Directive; or enter into a contract (or extend or renew a contract) with an entity that processes, transmits, or stores State of Vermont data using any product, service, system, or equipment referenced within this Directive. All State Agencies shall communicate this to applicable existing State of Vermont vendors within 30 days and direct those vendors to confirm their non-use of any of the products, services, systems, or equipment referenced within this Directive within 30 days of request receipt. Any reply from a vendor indicating their use of an identified product, service, system, or equipment referenced within this Directive shall be forwarded to the Secretary of Digital Services, via the CISO, and shall include a list of all State of Vermont technology or data affected using these products, services, systems, or equipment.
6. All requirements of this Directive may only be waived by the Secretary of Digital Services after receiving a request, endorsed by the Secretary or designated appointed authority of the requesting State Agency and the CISO, articulating the compelling justification for additional time to implement the requirements.
7. Internal point of contact for this Directive is Nicholas Andersen, State of Vermont Chief Information Security Officer, at nicholas.andersen@vermont.gov.

